Study Method

INFR11158/11230 Usable Security and Privacy

Dr. Jingjie Li

30/01/2024
Overview

• Reminder
• Cookie
• Study method
• Take-home
Blog submission

• Newly enrolled students please email TA (t.saka@sms.ed.ac.uk) and cc me for the first blog make up
Tutorials

- Tutorial 1: **Plan** a think-aloud study
- Tutorial 2: **Run** your planned think-aloud study and participant in someone else’s study
- Tutorial 3: **Plan and run** survey study
- Tutorial 4: **Analyze** the survey results
What is a cookie?

What does “opt-out” mean?
Designing the web cookie

Heavily based on Lou Montulli’s “The reasoning behind Web Cookies”
The year is 1994 and there is a problem... the internet has no ability to remember a person between page reloads.
There is an obvious easy solution...

Give each browser a unique identifier that gets sent with every page request.

My name is Bob

Hi Bob.

Hi new person, what is your name?

Hello web server my ID is 1234

1 day later

Hello web server my ID is 1234

Hi Bob, would you like to buy the shoes you looked at yesterday?
The problem with the obvious solution is privacy. Tracking would be possible with no visibility or control.
Instead Netscape implemented cookies. Small text strings the server could ask the browser to remember and give back to it later.

My name is Bob

Hi new person, what is your name?

Hi Bob. Please set a cookie with “Bob” as the string.

Hello web server

Hi Bob. Please set a cookie with “Bob” as the string.

Hello web server

Hi new person, what is your name?

Hi Bob, would you like to buy the shoes you looked at yesterday?

Hello web server

Hello web server 2

Hi new user. What is your name?

1 day later
Who is tracking you?
3rd party cookie reasoning

“Any company that had the ability to track users across a large section of the web would need to be a large publicly visible company.

Cookies could be seen by users so a tracking company can't hide from the public.

In this way the public has a natural feedback mechanism to constrain those that would seek to track them.”

-- Lou Montulli
Websites are made up of many elements from many sources
Sites I went to intentionally

All the △ are trackers or content sources contacted by the main site.
Third party cookies

adservice.google.com
GPS is Doomed (No Joke)

The World Economy runs on GPS. It needs a backup plan.

Take your pick: Linux on Windows 10 hardware, or Windows 10 on Linux hardware
We can’t see the Arm in having a little tinkerer

Pandas so useless they just look at delicious kid who fell into enclosure
Ugh, you’re infuriating!

A once-in-a-lifetime Opportunity: NASA bids emotional farewell to its cocky, hardworking RC science car on Mars
Amazing what you can achieve on unforgiving dust world over 15 years with a 20MHz RISC CPU and a bunch of probes

Oh Snap! Gimme-root-now security bug lets miscreants sock it to your Ubuntu boxes
Get an update, or risk giving a dodgy user or malware an upgrade

Request URL: https://tags.bluekai.com/site/4538?id=03F...
Request Method: GET
Status Code: 200 / OK

Request Headers
Accept: image/png, image/svg+xml, image/*; q=0.8, */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US, en; q=0.5
Connection: Keep-Alive
Cookie: bkdc=phx; bku=5LD99vg/jP0PYpyb
Host: tags.bluekai.com
Referer: https://stags.bluekai.com/site/50134?ret=html&...
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
So I went to BlueKai’s opt-out page and asked to opt-out.

Doing so set a cookie so that the next time I visit a site using BlueKai tracker the cookie tells the site not to track me.
Oracle's BlueKai tracks you across the web. That data spilled online

Billions of records exposed.

Zack Whittaker  @zackwhittaker / 3:30 PM GMT+1 • June 19, 2020
### BEFORE OPT-OUT

<table>
<thead>
<tr>
<th>Headers</th>
<th>Body</th>
<th>Parameters</th>
<th>Cookies</th>
<th>Timings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request URL: <a href="https://tags.bluekai.com/site/4538?id=03F">https://tags.bluekai.com/site/4538?id=03F</a>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Request Method: GET</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status Code: 200 / OK</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Request Headers
- Accept: image/png, image/svg+xml, image/*; q=0.8, */*;
- Accept-Encoding: gzip, deflate, br
- Accept-Language: en-US, en; q=0.5
- Connection: Keep-Alive
- **Cookie: bkdc=phx; bku=5LD99vg/jP0YPpyb**
- Host: tags.bluekai.com
- Referer: https://tags.bluekai.com/site/50134?ret=html&...
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)...

### AFTER OPT-OUT

<table>
<thead>
<tr>
<th>Headers</th>
<th>Body</th>
<th>Parameters</th>
<th>Cookies</th>
<th>Timings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request URL: <a href="https://stags.bluekai.com/site/50134?ret=h">https://stags.bluekai.com/site/50134?ret=h</a>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Request Method: GET</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status Code: 200 / OK</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Request Headers
- Accept: text/html, application/xhtml+xml, application/xml...
- Accept-Encoding: gzip, deflate, br
- Accept-Language: en-US, en; q=0.5
- Connection: Keep-Alive
- **Cookie: bku=0000000000000000; BKIgnore=1; bkdc=phx**
- Host: stags.bluekai.com
- Referer: https://www.nytimes.com/
- Upgrade-Insecure-Requests: 1
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)...

BTW, why “cookie”? 

• “Magic cookie”: a token or short packet of data passed between communicating programs

• (Web) cookie
Opting out causes the page to set an “opt out” cookie that is typically blank or all 0’s.

Instead of sending a cookie with a tracking number, your browser will now instead send the blank cookie, preventing the site from tracking you.
Is opt-out a one-stop solution?
Welcome to the BBC

LIVE Pentagon names three US soldiers killed in Jordan attack

Weekly fast is important discipline for me - Sunak

King leaves hospital as Kate recovers at home

How to stack your dishwasher, according to an expert

'100-year-old veteran's 'birthday walk' stops traffic

'Ratatouille restaurant' loses £1.3m-worth of wine

Sport headlines

Keep up with the latest from BBC Sport

We use cookies to give you the best online experience. Please let us know if you agree to all of these cookies.
Why we need to conduct a study?

- **Assess needs**: what should we build?
- **Examine trade-offs**: which features/approaches best fit needs?
- **Evaluate**: are requirements met? what can we improve?
- **Finding root causes**: what underlying problems need to be fixed?
Why we need to conduct a study?

• **Assess needs**: a better cookie notice?
• **Examine trade-offs**: which placement is more accessible?
• **Evaluate**: how fast/accurate people do opt-out?
• **Finding root causes**: dark pattern?
Why we need to conduct a study?

• Assess needs
• Examine trade-offs
• Evaluate
• Finding root causes

CMU USEC
Project lifecycle

What is wanted/needed → Analysis → Design → Implement and deploy

Prototype
Before we actually start

- Identify research questions
- Decide on the type of study and demographics
- Design study protocol
- Obtain ethics approval
- Design study
- Pilot studies
- Revise study....
Ethics guidelines

Ethics procedure

An overview of the School’s ethics procedure, including when and how to complete an ethics application for review.

Consideration of the ethical aspects of our research is both a moral and a legal obligation, as well as part of the academic culture in which we should be training researchers. The following procedures should help us fulfill those requirements. The goal of the system is full legal accountability with minimal effort. The first goal is served by keeping the full record. The second goal is served by keeping form filling to a minimum, by holding information locally, and by assuring that decision-making is as close to the pertinent research expertise as possible.

The procedures proposed here aim to ensure that ethical consideration are taken into account in any research done in the School. The proposed framework borrows heavily from current practice in PPRS Psychology and Linguistics, as well as procedures in Geosciences.

The system outlined on these pages apply to UG final year projects, MSc projects, PhD projects, Post-doc fellowships, funded research requiring a proposal, research performed by a visitor, and personal research for which there is no proposal.

Ethics application via online form

This is the online form, which has replaced the old Word forms. Please use it for all staff and student projects. Your data is stored on a server in the EU, following UK GDPR rules. The Principal Investigator will receive a copy of the form.

If you are submitting more than one ethics application, please wait to receive the automated confirmation of receipt for your first application before submitting the next.

Once submitted, the panel will aim to reply within 10 working days.

Update for December 2023 / January 2024:
Testing Usability…How?
Many ways to test usability

- A/B Testing
- Affinity Diagraming
- Card Sorting
- Case Studies
- Cognitive Walkthrough
- Competitive Testing
- Critical Incident Technique
- Customer Experience Audit
- Desirability Testing
- Diary Studies
- Ergonomic Analysis

- Experience Sampling
- Experiments
- Eye tracking
- Fly-on-the-wall Observation
- Focus Groups
- Graffiti Walls
- Heuristic Evaluation
- Interviews
- KJ Technique
- Observation
- Participatory Action Research
Behavioral – measures how people actually behave, what they do.

Attitudinal – measures what people say they think or how they say they behave.
Qualitative – unstructured data such as natural language.

Quantitative – numerical data. Anything that can be counted or measured with numbers.
Qualitative – unstructured data such as natural language.

Quantitative – numerical data. Anything that can be counted or measured with numbers.
Interviews – users express their attitudes by providing qualitative answers to questions.

Clickstream Analysis – measure the links users click on to get quantitative data on what users do.
Lab Studies – users perform a set of tasks often talking about their experience as they do so.

Surveys – Ask about user opinion often with multiple choice answers.
Think-pair-share

For each of the following problems, name one behavioral question you could ask and one attitudinal question.

• Mobile phone login
• Cookie dialogs
• Fake news
• Encryption of all webpages by default
Lab studies are a simple idea. You ask a user to come into a physical space and ask them to interact with the interface there.
Lab Study

• Basic idea: Have a participant come to a physical place (lab) and interact with the interface there
• You setup the lab so it mimics the situation you want to test
• Pros
  • Full control over the environment so limited confounds
  • Detailed data from each subject
  • Ability to ask them why they did something
• Cons
  • Small sample sizes
  • Being in the lab changes user behavior. They feel safer and their normal distractions are gone. That can be bad for deception studies.
Is it really simple?
What is different about security

- Large **information asymmetry** between participant and researcher
  - The researcher likely understand security of their tool
  - Participant likely doesn’t even know that security problem exists

- **Deception** studies are common
  - You told the participant to accomplish task A, but you are really looking to see if they do B activity
Why Johnny Can’t Encrypt:
A Usability Evaluation of PGP 5.0

Alma Whitten
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213
alma@cs.cmu.edu

J. D. Tygar
EECS and SIMS
University of California
Berkeley, CA 94720
tygar@cs.berkeley.edu

Abstract
User errors cause or contribute to most computer
security failures, yet user interfaces for security still
tend to be clumsy, confusing, or near-nonexistent. Is
this simply due to a failure to apply standard user
interface design techniques to security? We argue that,
on the contrary, effective security requires a different
usability standard, and that it will not be achieved
through the user interface design techniques appro priate
to other types of consumer software.

To test this hypothesis, we performed a case study
of a security program which does have a good user
interface by general standards: PGP 5.0. Our case
study used a cognitive walkthrough analysis together
with a laboratory user test to evaluate whether PGP 5.0
can be successfully used by cryptography novices to
achieve effective electronic mail security. The analysis
found a number of user interface design flaws that may

1 Introduction
Security mechanisms are only effective when used
correctly. Strong cryptography, provably correct
protocols, and bug-free code will not provide security if
the people who use the software forget to click on the
encrypt button when they need privacy, give up on a
communication protocol because they are too confused
about which cryptographic keys they need to use, or
accidentally configure their access control mechanisms
to make their private data world-readable. Problems
such as these are already quite serious: at least one
researcher [2] has claimed that configuration errors are
the probable cause of more than 90% of all computer
security failures. Since average citizens are now
increasingly encouraged to make use of networked
computers for private transactions, the need to make
security manageable for even untrained users has
become critical [4, 9].
If an average user of email feels the need for privacy and authentication, and acquires PGP with that purpose in mind, will PGP’s current design allow that person to realize what needs to be done, figure out how to do it, and avoid dangerous errors, without becoming so frustrated that he or she decides to give up on using PGP after all?
Users need to:

- understand that privacy is achieved by encryption, and figure out how to encrypt email and how to decrypt email received from other people
- understand that authentication is achieved through digital signatures, and figure out how to sign email and how to verify signatures on email from other people
- understand that in order to sign email and allow other people to send them encrypted email a key pair must be generated, and figure out how to do so
- understand that in order to allow other people to verify their signature and to send them encrypted email, they must publish their public key, and figure out some way to do so
- understand that in order to verify signatures on email from other people and send encrypted email to other people, they must acquire those people’s public keys
- manage to avoid such dangerous errors as accidentally failing to encrypt, trusting the wrong public keys, failing to back up their private keys, and forgetting their pass phrases
- be able to succeed at all of the above within a few hours of reasonably motivated effort
Tested usability using two methods

• Cognitive Walkthrough
  • A set of experts review the experts and make an informed guess about what will be problematic
  • Paired with heuristics – The experts state how the user interface supports or violates common HCI principles (Heuristics)

• Lab Study
  • Ask the participant to perform a set of tasks
  • Very similar to a think aloud, but without the talking aloud part
Cognitive walkthrough outcomes

- **Visual metaphors** – Do key and lock pictures make sense?
- **Different key types** – Public vs private keys, or maybe signing and encryption keys?
- **Key server** – Used for sharing keys
- **Key management policy** – Trust and validity ratings
- **Consistency** – Use of the same terms everywhere
- **Too much information** – Information like key size, hashes, and trust
- **Irreversible actions**
  - Accidentally deleting the private key
  - Accidentally publicizing a key
  - Accidentally revoking a key
  - Forgetting the pass phrase
  - Failing to back up the key rings
**Lab study**

- 12 participants with CS backgrounds
- Participant had to send several emails to team members (the researchers)
  - Creating a key pair
  - Sending their public key to team members
  - Getting team members’ public keys
  - Sending the email
  - Decrypting response email
- 3 – emailed the private key to the team member
  - 1 never realized the error
- 1 – forgot their pass phase and had to re-generate keys
- 1 – never figured out how to encrypt
- 7 – used their public keys to encrypt
  - 1 created a separate key pair for each team member
- 3 – successfully sent an encrypted email to the whole team and were able to decrypt an response email
Whitten and Tygar evaluated PGP encryption in 1999, surely it must be more usable now.
A personal story during my PhD

Kalêido: Real-Time Privacy Control for Eye-Tracking Systems

Jingjie Li, Amrita Roy Chowdhury, Kassem Fawaz, and Younghyun Kim
University of Wisconsin–Madison
{jingjie.li, roychowdhur2, kfawaz, younghyun.kim}@wisc.edu

Abstract
Recent advances in sensing and computing technologies have led to the rise of eye-tracking platforms. Ranging from mobiles to high-end mixed reality headsets, a wide spectrum of interactive systems now employs eye-tracking. However, eye gaze data is a rich source of sensitive information that can reveal an individual’s physiological and psychological traits. Prior approaches to protecting eye-tracking data suffer from two major drawbacks: they are either incompatible with the eye-tracking architecture or provide insufficient privacy guarantees.

Figure 1: Eye gaze heatmaps from an individual user with and without Kalêido’s noising effect on a web page.
Privacy Implications of Eye Tracking

Eye gazes from people with low social anxiety

Eye gazes from people with high social anxiety

Avoiding eye contacts as shown by the gaze locations
Some background

• Test out whether/how user experience is impacted by a privacy control we designed in an eye tracking game setting
How to do user studies?

My original plan in 03/2020 to do lab studies with a VR setup

Then...Guess what?
“The remote user study design was approved by the Institutional Review Board (IRB) of our institution... Each remote session took 35 minutes on average, and we provided each participant with $15 worth of supplies as a token of appreciation for participating.”
Questions
Take-home


• **(Blog)** BBC - [Google Chrome starts blocking data tracking cookies](https://www.bbc.com/sport/technology/56605559)